

Brief



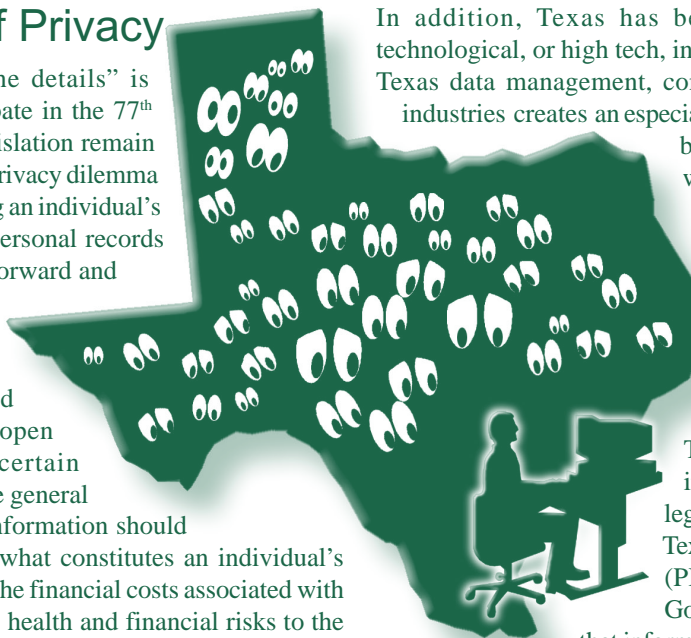
March 2001

Senate Research Center • Sam Houston Bldg. • Suite 575 • 201 E. 14th Street • Austin, TX 78701 • 512.463.0087 • Fax: 512.463.1271 • TDD: 800.735.2989

THE EYES OF TEXAS ARE UPON YOU: Gauging the Pulse of Privacy

The expression that “the devil is in the details” is particularly applicable to the privacy debate in the 77th Legislature. For the details of privacy legislation remain crucial to understanding and resolving the privacy dilemma facing legislators. On the surface, protecting an individual’s financial, medical, insurance, and other personal records from unsolicited inquiries seems straightforward and above dispute. Why, for instance, would concerns over individuals’ rights to determine who has access to their personal records be an issue? Why should personal information be accessible or open unless that person decides to make certain information available? While there may be general agreement that an individual’s personal information should be protected, there is disagreement over what constitutes an individual’s consent to releasing personal information, the financial costs associated with protecting individual information, and the health and financial risks to the individual and community if certain information is not disclosed. Balancing the market and government concerns of access to information and protecting individual personal information is exceedingly complex.

There are several general factors contributing to the privacy legislation debate in Texas. On a broad level, the Texas ethos of independence, individualism, and autonomy is a primary factor to consider in this debate. Texas is a state of independent residents. The Texas culture of individualism adds to this debate by protecting privacy interests at the same time it protects the economic pursuits of a market economy. In essence, the Texas political ethos is concerned with maintaining a minimal amount of government intervention into individual lives at the very time it urges government to protect civil and economic liberties, including an individual’s freedom from disclosing personal information.



In addition, Texas has become a leader in the technological, or high tech, industry. The growth of the Texas data management, computer, and e-commerce industries creates an especially challenging climate for balancing business interests with those of consumers. The locus of the debate centers on distinguishing between the self-regulatory nature of business and the necessity of government intervention to protect personal information.

Texas has also been a leader in passing open government legislation. For example, the Texas Public Information Act, (PIA) (Chapter 552, Texas Government Code) presumes that information in the possession of a government entity is public unless specifically exempted from disclosure by court order, under common law, under constitutional doctrine, or through a specific statutory exemption. Several of the exemptions to PIA reflect specific privacy concerns. For example, a number of statutory exemptions include prohibiting the disclosure of certain information contained in student records, private correspondence of an elected official, certain motor vehicle records, and certain medical records. In fact, the Texas Supreme Court has ruled that some types of information are confidential and exempt from the PIA. Such information includes highly intimate or embarrassing facts about a person’s private affairs such that its release would be highly objectionable to a reasonable person and that is of no legitimate concern to the public.

While strong open records laws provide safeguards against political abuse, they may lead to unnecessary disclosures of personal information. An important issue for legislators is delineating between information that is a “legitimate” concern to the public and information that a reasonable person would find highly objectionable.

Finally, the federal government has recently acted on the issue (see Federal Privacy Issue Brief) by requiring states to comply with certain minimal privacy levels in the areas of banking, consumer rights, and health information. In

“We face a growing privacy movement in this nation. It all but drowns out the voices of open government. This will have negative consequences.”

Rich Oppell, Editor *Austin American-Statesman* and President of the American Society of Newspaper Editors

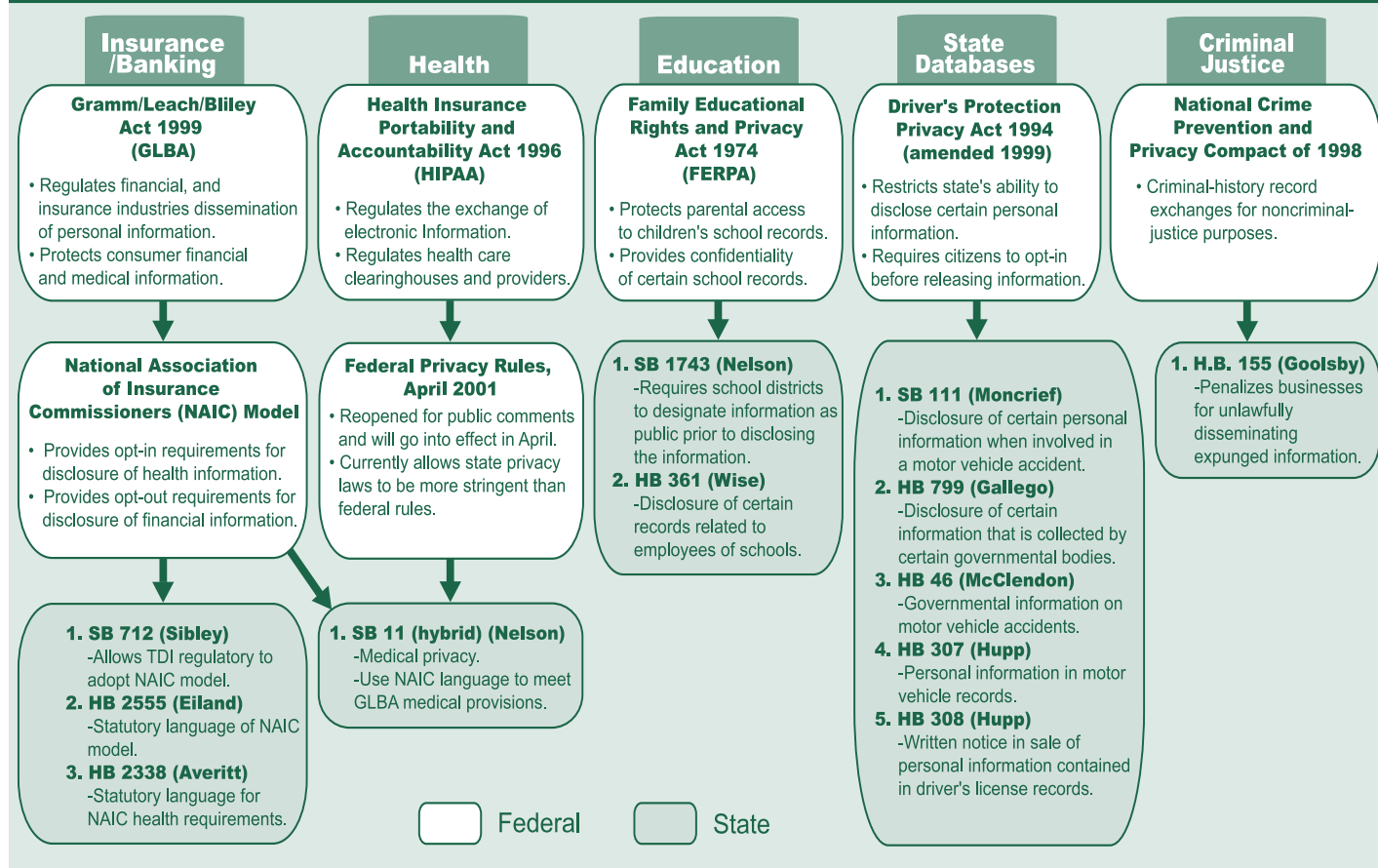


many cases, however, the federal laws place the onus of implementing and enforcing privacy laws on the states. In the areas of financial, insurance, and health information, states are granted a broad amount of latitude to establish privacy laws. Advocates for both consumers and industry are faced with devising rules that meet these concerns.

A diagram clarifying Federal laws and bills in the 77th Legislative session is below:

Interest groups acknowledge that the health privacy bill prevents the transfer of patient data from health entities to other marketing or advertising entities without a patient's consent, directs the state to adopt rules and establish penalties governing the release of patients specific data by health plans and insurance companies, gives patients the right to know how entities use their medical information in the form of an easy to understand public notice, establishes privacy standards for medical research efforts, and gives patients the right to inspect their medical records.

Links between Federal and State Privacy Legislation



HEALTH

The primary legislative debate on health privacy centered on S.B. 11, the Texas Medical Privacy Act, authored by Senator Nelson. The bill was engrossed by the Senate and now moves to the House. Basically, the legislation would prevent certain health care entities (the bill excludes insurers and employers unrelated to the health care industry) from releasing medical information to advertising or marketing entities without a patient's express consent. Additionally, patients would have the right to know how their medical information is being used and the right to sue an entity for releasing their information. The Office of the Attorney General (OAG) could impose a penalty of up to \$250,000 on those entities that fail to comply with the law.

Reactions to the bill, however, are mixed, with consumer and patient's advocacy groups at odds with insurance and business groups. The Texas Association of Health Plans (TAHP) is concerned with specific language in the bill. According to TAHP, the bill passed by the Senate could jeopardize the efforts of certain health plans to send notices and information about wellness checkups (i.e. remind enrollees of immunizations or well baby checkups or pregnancy checkups). As the bill currently reads, TAHP claims, health plans could violate those provisions of the bill that restrict certain promotional efforts when the patient has not given consent. Similarly, wellness checkups involving mailed reminder notices to enrollees of certain health plans would be a violation of the bill. TAHP stated that the organization is pursuing



an amendment to the bill that would allow health plans to contact patients in these examples. According to TAHP, legitimate health plan activities are excluded under the promotion clause of the bill.

The Texas Medical Association (TMA) disagrees with TAHP and strongly supports this legislation. According to TMA, well checkups are not excluded under the bill since this is considered a disease management issue. An amendment to the bill will not provide anything for disease management corporations and health plans. The bill does not exclude well checkup notices and other disease management activities.

The Texas Pharmacy Association (TPA) supports the current version of the bill. Pharmacists, under S.B. 11, will have the freedom to contact a customer on new drugs available to address their disease. The original bill, according to TPA, was too restrictive of pharmacists involved in disease management. Disease management protocols, as prescribed by physicians, combined with the role of the pharmacists, are an important part of patient health. The bill will not restrict this process.



The Texas Hospital Association (THA) notes that Texas hospitals already have strict confidentiality laws in place. While THA supports S.B. 11, they are concerned that the bill may prove difficult for hospitals, on a case by case basis, to apply the Health Improvement Portability and Accountability Act (HIPAA) or state law. It may prove challenging to determine whether HIPAA or state law is more stringent. One possibility to resolving this problem,

THA says, would be to clarify that those hospitals and other health entities meeting HIPAA guidelines meet state law as well. THA joins other organizations that express concerns with the marketing provisions of the bill. According to THA, they are concerned that the marketing provisions of the bill may interfere with hospitals' established disease management practices.

Consumers Union (CU) believes that one of the fundamental rights for individuals is the right to decide who may access an individual's personal information. Based on this premise, CU agrees with the concept of an opt-in approach (personal information is not disclosed, unless expressly released) to medical privacy.

According to CU, the version of S.B. 11 passed by the Senate goes beyond current federal health privacy rules, but does not provide adequate consumer protections. A primary concern of CU is that the bill does not contain state enforcement capabilities.

In addition, CU believes that the bill allows those entities under the bill to disclose medical information when it is part of "health care operations." CU claims that virtually everything in the medical field is covered under "health care operations." One element of the bill that CU suggests is consumer-oriented is a marketing

provision that will require an opt-in consent provision for covered entities before they can distribute advertising.

The Texas Life and Health Insurers Association (TLHIA) also supports the Senate version of the bill. The current version of the bill places medical privacy information collected by the insurers under the regulatory authority of the Texas Department of Insurance (TDI). Previous versions of the bill, TLHIA stated, had placed insurers under the regulatory authority of the Texas Department of Health. TLHIA stated that the bill essentially excludes insurers from being regulated by certain health-related provisions of the bill regarding the use and disclosure of personal information. The bill does lay out language for regulating the insurance industry's use of medical information by adopting statutory language consistent with the National Association of Insurance Commissioners (NAIC) model. However, TLHIA points out that the state must still comply with the consumer financial information provisions of the Gramm-Leach-Bliley Act (Financial Modernization Act) of 1999 (GLBA).

According to TLHIA, insurers are required to meet specific financial and medical privacy provisions in GLBA. S.B. 11 will serve as the state's medical component for insurance companies. However, TLHIA believes that protecting individual financial records will require additional legislation beyond S.B. 11. Three bills (S.B. 712, H.B. 2338, and H.B. 2555) are designed to meet the financial privacy component of GLBA.

FINANCE/BANKING/INSURANCE

GLBA allows banks, insurers, and securities dealers to share regulatory information among themselves that is confidential and privileged. This is vitally important in discerning important financial information among various affiliates and in determining the financial condition of insurers. GLBA sets a floor for financial information privacy, but explicitly permits states to enact more stringent standards of protection. Proponents of state insurance regulation contend that state-based standards better protect consumers. Yet, the new market place of financial modernization creates a conflict for state policymakers because state-regulated insurers' standards can be placed at a competitive disadvantage with federally regulated banks and securities firms. For example, banks and securities firms can use customer information to market new insurance products, while state laws may restrict insurers from using customer financial information to market other financial products.



Consumer advocates largely applaud the broader scope of the NAIC regulations, but favor more state and federal legislation to place "opt-in" requirements on third-party disclosures and restrict the sharing of financial information among affiliates.



The policy debate revolves around whether state legislatures: 1) should enact more stringent measures beyond GLBA; 2) should defer compliance with GLBA to the state insurance regulatory authority (TDI); or 3) defer to the federal guidelines in GLBA and remain silent on the issue.

S.B. 712, authored by Senator Sibley, includes those financial privacy conditions GLBA requires states to enact. The bill amends the Insurance Code by granting TDI rule-making authority to adopt certain requirements on privacy and disclosure of nonpublic personal financial information applicable to the insurance industry. TDI is expected to adopt the NAIC model to effectuate consistency for insurance companies and to comply with the federal regulations in GLBA. The commissioner of the TDI will be the rulemaking authority to adopt rules necessary to carry out and make the state eligible to override federal regulations.

In contrast, the companion bill in the Texas House of Representatives, H.B. 2555, sets the NAIC provisions of privacy as statutory language rather than allowing TDI rule-making authority relating to the details of financial privacy concerns.

The Independent Bankers Association (IBA) reported satisfaction with the recently amended version of S.B. 11 because it has a minimal impact on the billing and payment of health care and excludes payment activity from other limitations of GLBA. According to IBA, S.B. 11 follows language similar to HIPAA in excluding billing payment methods from stringent privacy provisions. Yet other banking associations feel Texas may not meet the higher privacy standards of other states, for example, the financial privacy laws of New York and California, often cited as model states for strong financial privacy. Currently, Texas is considering legislation that will conform to GLBA requirements. There is no current legislation exceeding those as exists in GLBA or making financial laws more stringent in the state.

EDUCATION

The Family Educational Rights and Privacy Act (FERPA) of 1974 protects both parents' access and confidentiality of educational records. FERPA controls the release of student scholastic information by educational institutions, requiring them to obtain permission from parents or students over 18 years old. Some states, including Texas, have adopted laws requiring schools to notify state agencies when a student drops out so that the student's driver's license may be revoked. Texas colleges and universities claim FERPA hinders their search for students who qualify for automatic admission as a result of belonging to the top 10 percent of their graduating classes. U.S. Department of Education officials and others argue that both uses of student records violate FERPA because they could result in unauthorized release of academic records to either withdraw a privilege (driver's licenses) or grant a benefit (automatic college admission). Texas law allows educational institutions to perform criminal history checks on all employees, volunteers, and prospective employees, as well as volunteers, employees and prospective employees of any entity contracting to provide services. Texas law requires the State Board

of Educator Certification (SBEC) to do a background check on any person applying for certification.

H.B. 361, filed this session by Representative Wise, would embellish existing law by requiring both SBEC and a school district to contact the Federal Bureau of Investigation (FBI) as well as "any law enforcement agency" to search federal databases for criminal history information. It would also allow SBEC and independent school districts to charge the applicant for the cost of the background checks. The bill would require all education entities to screen potential employees and volunteers by having them sign an affidavit that he or she has never been convicted of, pleaded guilty to, pleaded *nolo contendere*, or admitted to committing enumerated offenses. Since 1998, 20 states have added or amended laws allowing or requiring schools to perform criminal background checks for persons engaged in educational activities.

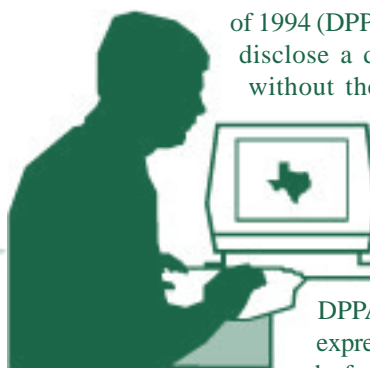
The Texas Association of Social Workers and the National Center for Missing and Exploited Children support H.B. 361 because they believe that the potential harm or risk to children outweighs the minimal harm of subjecting employees to background checks. The Texas State Teachers Association (TSTA), which opposed a similar bill last session, remains concerned that under the proposed legislation, a current employee would have to pay for a background check. TSTA is also concerned that the bill may violate an individual's civil liberties by subjecting individuals to an *a posteriori* background check when they are currently employed by school district.

STATE DATABASES

The Federal Driver's Privacy Protection Act of 1994 (DPPA) restricts the states' ability to disclose a driver's personal information without the driver's consent, generally

prohibiting the knowing disclosure of personal information about any individual obtained in connection with a motor vehicle record (MVR).

DPPA requires a state to obtain the express consent (opt-in) of the person before it releases personal



information for bulk distribution or any other use. Failure by a state to comply with this provision not only exposes a state to civil penalties, but can prevent the state from receiving federal funds for highway and other transportation projects. The amendment specifically provided that Texas has until 90 days during the next convening of the state legislature (the 77th Legislature) to comply with the new "opt in" requirements.

Rich Oppell, editor of the *Austin American-Statesman*, stated that the DPPA limits newspapers' access to driver's license records. According to Oppell, this could have negative consequences for open government. For example, Oppell stated, under DPPA newspapers can no longer use driver's license records to identify drunken drivers with revoked licenses. DPPA is another example,



PRIVACY BILLS IN THE 77TH TEXAS LEGISLATURE

Bills	Summary	Status (Date) and Actions Taken
Health Bills		
S.B. 11 (Nelson)	Protects the privacy of medical records.	Engrossed in Senate (3-21)
H.B. 1221 (Maxey)	Protects privacy of medical records.	In Public Health (2-08)
S.B. 12 (Nelson)	Prohibits use of certain medical information in determining employment.	Pending In Business and Commerce (3-20)
S.B. 13 (Nelson)	Prohibits use of certain medical information in determining insurance coverage.	In Business and Commerce (1-10)
S.B. 177 (Madla)	Use of electronic surveillance devices in nursing homes.	In Health and Human Services (1-11)
Protective Services		
S.B. 15 (Nelson)	Disclosure of information relating to victims of sexual assault.	Engrossed in Senate, in House Calendar
S.B. 27 (Shapiro)	Address confidentiality program for victims of family violence or stalking.	Pending in State Affairs (3-20)
State Databases		
S.B. 111 (Moncrief)	Protecting release of certain information relating to motor vehicle accidents.	In State Affairs (1-11)
H.B. 799 (Gallego)	Limits disclosure of certain personal information collected by certain governmental bodies.	In State Affairs (3-05)
H.B. 46 (McClendon)	Governmental information about motor vehicle accidents.	Pending in House Public Safety (3-19)
H.B. 307 (Hupp)	Disclosure of personal information from motor vehicle records.	Pending in State Affairs (3-05)
H.B. 308 (Hupp)	Written notice of the sale of personal information contained in driver's license record filed.	In State Affairs (1-29)
Business and E-Commerce		
H.B. 241 (Hupp)	Request for disclosure of an individual's social security number made by a business.	In State Affairs (1-25)
Criminal Justice		
H.B. 155 (Goolsby)	Expunction of arrest records from businesses publishing conviction or arrest information.	Pending In Criminal Jurisprudence (3-05)
Insurance		
S.B. 712 (Sibley)	Privacy of certain information provided by consumers to insurers and other entities.	Engrossed in Senate; Referred to House Insurance (3-20)
H.B. 338 (Averitt)	Disclosing information related to criminal activity, fraud, material representation, or nondisclosure in connection with an insurance transaction.	Pending in Insurance (3-05)
Education		
H.B. 361 (Wise)	Background checks on employees, volunteers, and prospective volunteers of educational institutions.	In Public Education (1-30)
General Privacy		
S.B. 867 (Nelson)	Joint interim task force to study various issues affecting personal privacy.	Engrossed in Senate (3-22)
S.B. 866 (Nelson)	Creating a Texas Privacy Act to address how government entities affect personal privacy.	Engrossed in Senate; Referred to House State Affairs (3-20)
H.B. 1922 (McCall)	Developing a state government privacy policy.	Substitute Reported to House Chamber (3-19)
H.J.R. 15 (Hupp)	Right of privacy constitutional amendment.	In State Affairs (1-24)

Oppell claims, of a diminished importance that society places on open government.

The Texas Department of Public Safety (DPS) has an “opt-out” procedure for collecting and distributing information (records are public, unless the consumer specifically requests that information

not be disclosed). DPS has testified that it annually generates approximately \$44 million in annual revenue from the sale of MVR information. However, this ‘opt out’ procedure now conflicts with the DPPA, which bars disclosure of such information unless the individual expressly consents to its release. Both DPS and the



Texas Department of Transportation are considering rules that would assure compliance with the new “opt in” provisions of the federal law.

Under H.B. 307, Representative Hupp’s bill, an agency could release personal information for other than specified governmental, legal, verification, or safety reasons only if the person who is the subject of a MVR has given written consent. H.B. 308 would amend the Transportation Code to require that DPS or an agency, any time it sells personal information from MVRs, provide the individual the information pertaining to notice of the sale and the identity of the purchaser. DPS would also establish a fee to be charged to purchasers of such information.

H.B. 799, by Representative Gallego, would amend the state’s public information laws (Chapter 552 of the Government Code) to limit the disclosure of certain personal information, including that contained in MVRs, by state agencies. The proposed changes regarding the disclosure of MVRs substantially incorporate portions of the DPPA, including the definition of “personal information.”

Texas law also covers information held by a governmental entity relating to a motor vehicle accident, including accident reports, dispatch logs, towing records, and the part of any other record that includes information relating to the date of the accident, the name of any person involved, or the accident’s specific location. Except as otherwise provided, this information is privileged and for the confidential use of federal and state governmental entities. It may be released, upon receipt of a written request and payment of any required fee, to certain government entities, law enforcement agencies; or a person who provides the name of any person involved in the accident and either the date of the accident or the specific address or the highway or street where the accident occurred.

Newspaper groups recently filed suit against the state asking for a judgment that traffic accident reports are separate from MVRs and are therefore not covered by the confidentiality requirements of Texas law. They asserted that the requirement that they provide the name of a person involved in the accident and date or location of the accident would make it difficult to report traffic accidents. The judge issued an order temporarily enjoining enforcement of these provisions regarding accident reports and, following a January 18, 2000 trial, indicated he would rule in favor of the newspapers. However, no final judgment and order was ever signed. It is possible that the newspapers are waiting to see if the legislature will amend the law this session.

S.B.111, authored by Senator Moncrief, makes motor vehicle accident information public and authorizes its release, but bars governmental entities from disclosing information related to motor vehicle accidents to any person unless the person affirms that the information will not be used for the direct solicitation of business or employment for pecuniary gain by certain persons. There is also a penalty for using such information to solicit business from accident victims. On the other hand, H.B. 46 by Representative McClendon would include all information relating to a motor

vehicle accident, other than an accident report held by a governmental entity to remain private.

State law expressly excludes “information on vehicular accidents” from the definition of personal information. However, it is not clear whether this refers to information about the accident itself (such as date or location) or also includes specific information about the person involved in the accident (e.g. name, address). There are no federal rules interpreting this section, and, because the states and other interested parties are waiting for the United States Supreme Court to rule on the constitutionality of the DPPA, there have been



**“The cameras
are coming.
We are not
going to
stop them.
An open
society is not
only going
to be
more free,
it’s going
to protect
that special
reserve of
privacy we
all need.”**

—David Brin,
Transparent Society



no court decisions regarding the interpretation of various provisions of the Act. DPS has indicated that it considers such information separate from MVRs and therefore not covered under DPPA.

PROTECTIVE SERVICES



Address confidentiality for victims of domestic violence

When victims of domestic violence leave an abusive situation and establish new homes, it is often critical that abusers not be able to find their victims. However, this veil of anonymity can be threatened if the victims' home, work, and school addresses appear in open governmental records. Currently, victim address information found in court records and the addresses of family violence shelters are commonly kept confidential. A general concern remains accommodating victims in a way that will allow them to apply for social services or exercise their right to vote without exposing themselves to discovery through public records. Ten states (California, Florida, Illinois, Nevada, New Hampshire, New Jersey, Rhode Island, Vermont, Washington, and Wisconsin) have enacted some type of address confidentiality program. Most of these states allow people to apply for the address confidentiality program if the applicants swear that they are victims of domestic violence. Several require verification of this statement through court, police, or social service records. Most states run their programs through either the secretary of state or the office of the attorney general. The lead agency provides an alternate address to be used by victims when they are required by local or state governmental agencies to give an address for services. The lead agency forwards the victim's mail to the victim's actual address.

Thus the actual address does not become part of the governmental records subject to open records requests. Most states either allow an application for or automatically send a program participant an absentee ballot.

Bills (S.B. 15, S.B. 27) have been filed with the 77th Legislature that establish an address confidentiality program for victims of family violence or stalking to be administered through the secretary of state. These bills also exempt personal victim information gathered at family violence shelter centers and through sexual assault programs from being subject to open records requests.

PRIVACY PROTECTION AND THE EXPUNCTION OF CRIMINAL RECORDS

Guaranteeing the privacy of expunged information is proving to be a challenge for the state as commercial resellers and Internet data compilers purchase information under PIA and sell it for profit over the Internet on a daily basis. Acknowledging administrative limitations, DPS, court clerks, and law enforcement agencies are currently examining the regulations that govern expunction to determine whether improved guidelines and enforcement mechanisms are needed.



Expunction is the legal process by which, upon request by the defendant, the court may order the records of a criminal conviction to be physically destroyed or sealed from files, computers, and other depositories. In some states, expunction is also available for persons unlawfully arrested or not ultimately convicted. Individuals most often need a clean criminal history in order to have access to housing, employment, education, and licensure. By having their criminal records expunged, individuals can deny an arrest and existence of expunction order unless under oath in a criminal proceeding. Under oath, an individual must legally represent that some offenses they committed have been expunged.

Juveniles who have some form of history with the juvenile justice system may also seek to have their records expunged. While acknowledging the reality of youthful mistakes, some juvenile advocates do not believe the consequences of having a criminal record should follow adolescents throughout their adult lives.

Forty-nine states, including Texas, provide for some type of process that purges individual criminal records. Chapter 55 of the Texas Code of Criminal Procedure (CCP) governs the expunction of criminal records. DPS maintains Texas' statewide criminal information database system, receiving over 4,000 petitions for expunction every year.



While individuals may think that they have followed procedures to have their records properly expunged, previously existing criminal information may have already found its way into databases in cyberspace, accessible to anyone. Once information is collected into these databases, little if anything is being done to assure the accuracy of the information, including updating the database to delete expunged criminal history records. PublicData.com, a company that collects public records, states that it is not responsible for any inaccuracies in any database. This company maintains a web site that enables customers to search a multitude of databases containing compiled information on individual criminal, sex offender, driver's license, voter, civil court, license plate, vehicle ID, professional, and federal records.

Anyone running on-line background checks with the goal of providing a safe working, learning, or living environment may not necessarily receive the most accurate information on individual applicants. For example, there are instances where landlords, perspective employers, institutions of learning, and professional licensing boards reject applicants based on criminal records that were to be expunged. (As of 1999, DPS's on-line conviction database recorded over 1.4 million hits per month).

Opponents to limiting the dissemination and use of criminal history information question the degree to which the state should control how people share information. Eugene Volokh, a law professor at

the University of California at Los Angeles, explains, "the right to control information about ourselves sounds appealing until you realize it's the right of others to speak about us." Many fear that excessive governmental intervention could inflict serious damage to the economic advance of the information age and could result in fewer services for consumers. Commerce, trade, and consumer advocates prefer laws that balance the privacy rights of citizens with the rights of businesses to freely exchange information.

During the Interim before the 77th Legislature, court clerks and law enforcement agencies testified to additional problems with the internal maintenance of criminal history records. Each cited a variety of administrative difficulties arising due to time pressures, lack of adequate notice of hearings, and inadequate delivery of expunction petitions specifying which records to delete. The Senate Committee on Criminal Justice, in its Interim Report to the 77th Legislature, responded with recommendations to improve the administrative efficiency of Chapter 55 of the CCP.

Currently, members of both the House of Representatives and the Senate have filed 20 bills related to expunction. The majority of these bills are aimed at expanding the eligibility requirements that determine who may have criminal history records expunged. Only one bill directly addresses the issue of increased privacy protection. H.B. 155, by Representative Goolsby, seeks to specifically penalize businesses unlawfully disseminating expunged information. H.B. 155 would amend Article 55.02 of the CCP to require "all persons in the business of publishing or disclosing conviction or arrest information to be included in the expunction petition." This bill would also amend Section 411.135 of the Texas Government Code and make it a Class B misdemeanor for "a person in the business of publishing or disclosing conviction or arrest information to knowingly use or release arrest information that is the subject of an expunction order."

—by Senate Research Center
Rita Aguilar
Dunya Bean
Tammy Edgerly
Betsy Heard
David Thomason
Sharon Weintraub